

WHAT IS CLAIMED IS:

1. A cryptographic system in a computer system, comprising:

at least one server; and

at least one secret value including a master key, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key, the parts being encrypted by a password-derived or token-based key, each part being associated with a password wherein the at least one server can update the master key by requiring only some of the passwords to be revealed.

2. A cryptographic system as in claim 1, wherein the master key is used for protecting sensitive information processed by the at least one server.

3. A cryptographic system as in claim 1 further comprising a database, wherein the sensitive information is stored in the database.

4. A cryptographic system as in claim 1 in which the master key is split into the two or more parts according to the Bloom-Shamir methodology.

5. A method used in a cryptographic system, comprising:

providing at least one secret value including a master key;

splitting the master key into two or more parts wherein fewer than all the parts are required for reassembling the master key; and

encrypting the parts by a password-derived or token-based key, each part being associated with a password, wherein the master key can be reassembled by requiring only some of the passwords to be revealed.

Figure 1 consists of 12 sub-diagrams labeled (a) through (l), arranged vertically. Each diagram shows a different stage in the construction of a 3D model of a human head and neck. (a) shows a basic wireframe of the head and neck. (b) through (l) show the model being refined with more detail, including facial features like eyes, nose, mouth, and ears, and the addition of skin shading and texture. The diagrams are arranged in a column, with each subsequent diagram building upon the previous one.